

**IN THE UNITED STATES DISTRICT COURT  
FOR THE WESTERN DISTRICT OF NORTH CAROLINA  
CHARLOTTE DIVISION  
CIVIL ACTION NO. 3:20-CV-00690-FDW-DSC**

**ETHAN DARNELL,**

**Plaintiff,**

**v.**

**WYNDHAM CAPITAL MORTGAGE,  
INC.,**

**Defendant.**

**ORDER**

THIS MATTER is before the Court on Defendant Wyndham Capital Mortgage's Motion to Dismiss. (Doc. No. 12). The motion has been fully briefed by the parties and is now ripe for review. For the reasons stated herein, the Court GRANTS Defendant's Motion to Dismiss.

**I. BACKGROUND**

Plaintiff filed his Class Action Complaint against Defendant Wyndham Capital Mortgage on December 10, 2020. (Doc. No. 1). He asserts multiple causes of action against Defendant for Defendant's alleged failure to secure Plaintiff's, and others', personally identifying information ("PII"). Id. The following allegations are taken as true for purposes of this Order and are set forth as described in the Complaint.

Defendant Wyndham is a nationwide mortgage provider incorporated in North Carolina. (Doc. No. 1). Defendant uses "'advanced technology' for its strictly online loan processes in an effort to streamline" the mortgage loan process. Id. at p. 1. Plaintiff is a Florida citizen and allegedly applied for and received a home loan from Defendant in January of 2020. Id. He subsequently refinanced his loan with Defendant in July of 2020, and shortly thereafter Defendant allegedly "sold" Plaintiff's mortgage loan to another company. Id. at p. 3.

Sometime after Plaintiff's loan with Defendant was sold, Defendant sent multiple "Notice of Data Incident" messages to "numerous states' Attorneys General." Id. at p. 5. The first Notice was sent on or around October 16, 2020:

This correspondence is to notify you of [a] potential security issue caused by a recent single occurrence of user error. On September 18, 2020, an email containing personal information was sent in error to an email account not belonging to [Wyndham]. [Wyndham] has no evidence that this email was opened or that the information has been used. Upon identifying the incident, [Wyndham] immediately took action to address the problem, including an attempted recall of the email and attempted communications to the mailbox owner and service provider to have the email deleted. [Wyndham] has put additional protections in place to keep this from happening again, has provided additional training to employees, and continues to strengthen system controls and monitoring.

Id.

A second Notice was sent to various Attorneys General roughly one week later, on or around October 23, 2020:

This correspondence is to notify you of [a] potential security issue caused by a phishing scam. [Wyndham] discovered that an employee was the victim of a phishing scam which allowed access to the employee's email account for a limited period of time. Upon discovery, [Wyndham] took immediate action; [Wyndham] blocked the unauthorized access, changed passwords and launched an investigation. In response to this incident, [Wyndham] has put additional protections in place to keep this from happening again, has provided additional training to employees, and continues to strengthen system controls and monitoring.

Id.

Plaintiff alleges he received a similar Notice of Data Breach on or around October 16, 2020.<sup>1</sup> Id. at p. 3. In the Notice sent on October 16, 2020, Defendant explained that it would offer "affected individuals one year of credit monitoring" and recommended that all those potentially impacted closely monitor their financial accounts for "suspicious activity." Id. at pp. 6-7. Plaintiff alleges that, once he was made aware of the data breach, he began to monitor his financial accounts

---

<sup>1</sup> Plaintiff has not provided a verified copy of the Notice he allegedly received, and the Court accordingly relies on only the allegations contained in the Complaint. It is unclear from the Complaint whether the Notice sent to Plaintiff was in reference to the breach flowing from the accidental email or in reference to the breach flowing from the phishing scam.

and has spent “additional time routinely reviewing his credit monitoring service results and reports,” which is time he could spend on other leisure or professional activities. Id. at p. 7. He alleges he has been suffering from “great anxiety” as a result of the data breach and specifically alleges the following injuries: “(a) damages to and diminution in the value of his PII—a form of intangible property that the Plaintiff entrusted to [Defendant] as a condition of his employment; (b) loss of his privacy; and (c) imminent and impending injury arising from the increased risk of fraud and identity theft.”<sup>2</sup> Id. at pp. 7-8.

As recourse for his alleged injuries,<sup>3</sup> Plaintiff seeks to hold Defendant liable for (1) negligence; (2) violating Florida’s Unfair and Deceptive Trade Practices Act; (3) unjust enrichment; (4) breach of implied contract; (5) breach of confidence; and (6), seeks a declaratory judgment that Defendant’s data security protocols are insufficient as a matter of law. (Doc. No. 1). Defendant has moved to dismiss both for lack of standing and for failure to state a claim.<sup>4</sup>

## **II. LEGAL STANDARD**

### **a. Subject Matter Jurisdiction**

Rule 12(b)(1) provides for dismissal of claims against all defendants where the Court lacks jurisdiction over the subject matter of the lawsuit. Lack of subject matter jurisdiction may be raised at any time either by a litigant or the court. Mansfield, C. & L.M. Ry. Co. v. Swan, 111 U.S. 379, 382 (1884). The Federal Rules of Civil Procedure provide that “If the court determines

---

<sup>2</sup> Plaintiff references his “employment” with Defendant. The Court assumes this was written in error as there are no other allegations about Plaintiff’s employment with Defendant elsewhere in the Complaint.

<sup>3</sup> Plaintiff alleges injuries on behalf of himself and the alleged class members. However, for purposes of this Order, the Court’s legal analysis is based only on the named Plaintiff’s alleged injuries. See Beck v. McDonald, 848 F.3d 262, 269 (4th Cir. 2017) (“In a class action, we analyze standing based on the allegations of personal injury made by the named plaintiffs.” (citation omitted)).

<sup>4</sup> For the reasons stated herein, the Court declines to address Defendant’s argument that Plaintiff has failed to state a claim.

at any time that it lacks subject-matter jurisdiction, the court *must* dismiss the action.” Fed. R. Civ. P. 12(h)(3) (emphasis added).

Subject matter jurisdiction may be challenged in one of two ways: either facially or factually. See Kerns v. United States, 585 F.3d 187, 192 (4<sup>th</sup> Cir. 2009). On the one hand, a facial challenge occurs when a defendant asserts that “a complaint simply fails to allege facts upon which subject matter jurisdiction can be based” and requires a court to accept as true the factual allegations in the complaint. Id. (quotation omitted). On the other hand, a factual challenge occurs when a defendant “argues that the jurisdictional allegations in the complaint [are] not true,” and allows a court to conduct a hearing and disregard the allegations in the complaint if appropriate. Beck v. McDonald, 848 F.3d 262, 270 (4<sup>th</sup> Cir. 2017) (quotation and citation omitted).

Regardless of whether challenged facially or factually, when a court considers subject matter jurisdiction, the burden of proof is on the plaintiff. Adams v. Bain, 697 F.2d 1213, 1219 (4<sup>th</sup> Cir. 1982). In Richmond, Fredericksburg & Potomac R.R. Co. V. United States, 945 F.2d 765 (4<sup>th</sup> Cir. 1991) (Ervin, C.J.), the Court of Appeals for the Fourth Circuit held as follows:

In determining whether jurisdiction exists, the district court is to regard the pleadings' allegations as mere evidence on the issue[] and may consider evidence outside the pleadings without converting the proceeding to one for summary judgment. The district court should apply the standard applicable to a motion for summary judgment, under which the nonmoving party must set forth specific facts beyond the pleadings to show that a genuine issue of material fact exists. The moving party should prevail only if the material jurisdictional facts are not in dispute and the moving party is entitled to prevail as a matter of law. A district court order dismissing a case on the grounds that the undisputed facts establish a lack of subject matter jurisdiction is a legal determination subject to de novo appellate review.

Id. at 768-69 (citations omitted).

### **III. STANDING**

When standing is challenged facially, the court must “accept as true all material allegations of the complaint and construe the complaint in favor of the complaining party.” Deal v. Mercer

Cty. Bd. of Educ., 911 F.3d 183, 187 (4th Cir. 2018) (citing S. Walk at Broadlands Homeowner's Ass'n, Inc. v. OpenBand at Broadlands, LLC, 713 F.3d 175, 181-82 (4th Cir. 2013)). Article III standing requires a plaintiff to demonstrate “(1) that he or she suffered an injury in fact that is concrete, particularized, and actual or imminent; (2) that the injury was caused by the defendant, and (3) that the injury would likely be redressed by the requested judicial relief.” Thole v. U.S. Bank N.A., — U.S. —, 140 S. Ct. 1618, 1618, 207 L. Ed 2d 85 (2020). Defendant takes issue only with the first standing requirement—injury in fact—and the Court accordingly directs its analysis.

The Fourth Circuit has recently addressed the injury in fact requirement in the data breach context in Beck v. McDonald, 848 F.3d 262 (4th Cir. 2017) and in Hutton v. Nat. Bd. of Examiners in Optometry, Inc., 892 F.3d 613 (4th Cir. 2018). When read together, both cases hold that, in the Fourth Circuit, a plaintiff has suffered a legally cognizable injury from a data breach in which PII may have been compromised when there is either “actual injury of identity theft; or . . . a threatened injury based on substantial risk of future identity theft that is sufficiently imminent.” In re Marriot Int'l, Inc., Customer Data Sec. Breach Litig., No. 19-md-2879, 2020 WL 6290670, at \*4 (D. Md. Oct. 27, 2020) (citing Hutton, 892, F.3d 613, 622); Beck, 848 F.3d at 275-76.

In Beck, the Fourth Circuit reviewed a consolidated appeal brought by veterans who, after receiving medical care at a Veterans Affairs Medical Center (“VA Center”), were made aware of a data breach in which their personal information was compromised. Beck, 848 F.3d at 266. The data breach occurred when a laptop with the “unencrypted personal information” of thousands of patients was “misplaced or stolen” from the VA Center. Id. at 267. The plaintiffs alleged they were injured and sought to establish standing based on the “increased risk of future identity theft and the cost of measures to protect against it.” Id. at 267. The district court held that the plaintiffs

“failed to establish a non-speculative, imminent injury-in-fact for purposes of Article III standing.”<sup>5</sup> Id.

The Fourth Circuit affirmed, finding that neither alleged injury—the increased risk of future identity theft nor the costs of protecting against future identity theft—was sufficiently imminent to satisfy Article III’s requirement that a threatened injury be “certainly imminent” to constitute injury-in-fact. See id. at 270-73 (discussing and applying Clapper v. Amnesty Int’l USA, 568 U.S. 398 (2013)). With respect to the first alleged injury, increased risk of future identity theft, the Fourth Circuit reasoned in part that because the plaintiffs failed to allege the laptop was stolen “with the intent to steal [plaintiffs’] private information,” the possibility of future identity theft was too attenuated to confer Article III standing. See Beck, 848 F.3d at 274-75. The possibility of future identity theft was too attenuated because the court had to

assume that the thief targeted the stolen items for the personal information they contained. And . . . [that] the thieves must then select, from thousands of others, the personal information of the named plaintiffs and attempt to successfully use that information to steal their identities. This “attenuated chain” cannot confer standing.

Id. at 275. With respect to the second alleged injury, the cost of measures taken to prevent future identity theft, the Fourth Circuit found that “self-imposed harms cannot confer standing.” Id. at 277 (quoting Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 694 (7th Cir. 2015) (“Mitigation expenses do not qualify as actual injuries when the harm is not imminent.”)). Accordingly, under Beck, allegations of a data breach causing a future threat of identity theft, without more, cannot confer standing without factual allegations plausibly suggesting “that the threatened harm of future identity theft [is] ‘certainly impending.’” Beck, 848 F.3d at 275. Otherwise, an alleged injury of future identity theft is too attenuated to be sufficiently imminent.

---

<sup>5</sup> Two of the plaintiffs appealed the district court’s grant of summary judgment in favor of the defendant because the plaintiffs did not have Article III standing. Beck, 848 F.3d at 267. The other plaintiffs appealed the district court’s dismissal of the complaint for lack of Article III standing. Id. at 269.

In Hutton, the Fourth Circuit reviewed a consolidated appeal brought by a group of optometrists who realized their personal information was stolen from databases maintained by the National Board of Examiners in Optometry (“NBEO”) after the optometrists noticed that credit cards were fraudulently opened in their names.<sup>6</sup> Hutton, 892 F.3d at 616. The named plaintiffs alleged the same injuries as in Beck: increased risk of future identity theft and the cost of monitoring for such theft. See Hutton, 892 F.3d at 619. The district court relied on Beck and dismissed the complaint for lack of standing, in part because the plaintiffs had failed to sufficiently allege threat of imminent injury.<sup>7</sup> Id.

The Fourth Circuit reversed the district court’s dismissal. Id. at 616. The court reaffirmed the basic rule set forth in Beck: that the “mere compromise of personal information, without more, fails to satisfy the injury-in-fact element in the absence of an identity theft.” Hutton, 892 F.3d at 621 (quoting Beck, 848 F.3d at 274-75). However, the court explained that the plaintiffs in the present case had suffered *actual* harm when credit cards were fraudulently opened in their name. Hutton, 892 F.3d at 622. There was “no need to speculate on whether substantial harm will befall the [p]laintiffs.” Id. Accordingly, under Hutton, a data breach may confer standing when a plaintiff alleges “that [his or her] data has been stolen, accessed, and used in a fraudulent manner.” Id.

Here, Plaintiff has alleged actual injury in the form of “(a) damages to and diminution in the value of his PII; (b) loss of his privacy; and (c) imminent and impending injury arising from the increased risk of fraud and identity theft.” (Doc. No. 1, pp. 7-8). Defendant argues that none

---

<sup>6</sup> The optometrists who had credit cards fraudulently opened in their names realized the common thread among them was that they had all, at some point, shared their personally identifying information with the NBEO. Hutton, 892 F.3d at 617.

<sup>7</sup> The district court also determined the plaintiffs’ alleged injuries failed the causation requirement of standing. Hutton, 892 F.3d at 619.

of the alleged injuries are sufficient to confer Article III standing; each alleged injury will be addressed in turn.

**a. Damages to and Diminution in Value of PII**

Plaintiff first alleges injury in the form of “damages to and diminution in the value of his PII” as a result of having his “PII exposed.” (Doc. No. 1, p. 7). It is not clear from the Complaint exactly how the exposure of Plaintiff’s PII has damaged or diminished its value, but the Court assumes that, because PII is of “high value to criminals,” Plaintiff is prevented from realizing the full extent of his PII’s value if it has been potentially exposed to cyber criminals. See id. at pp. 8-11.

“The Fourth Circuit has not [explicitly] decided whether the loss of property value in [PII] constitutes a cognizable injury in data breach cases.” In re Marriott Int’l, Inc. Customer Data Sec. Breach Litig., 440 F. Supp. 3d 447, 460 (D. Md. 2020). However, both Beck and Hutton foreclose the possibility that the exposure of PII, without more, is sufficient to confer Article III standing. See Kimbriel v. ABB, Inc., No. 5-19-cv-215-BO, 2019 WL 4861168, at \*3 (E.D.N.C. Oct. 1, 2019) (citing Hutton, 892 F.3d at 621 (“[Beck] emphasized that a mere compromise of personal information, without more, fails to satisfy the injury-in-fact element in the absence of identity theft.”)). Here, the allegations as set forth in the Complaint do not sufficiently allege the “something more” required to satisfy the standards as outlined in Beck and reaffirmed in Hutton. And while the Court declines to speculate on the kinds of factual allegations that could serve as “more,” Plaintiff does not allege *anything* more than the “mere compromise” of his PII, which is clearly insufficient under Beck and Hutton.

The Court’s conclusion is further supported by the cases referenced by Plaintiff in his Opposition Motion, all of which involved the actual misuse of PII or allegations of something



more than the mere exposure of PII. See In re Marriot International, Inc., 440 F. Supp. 3d at 460-62 (“Plaintiffs allege that they suffered lower credit scores as a result of the data breach and that fraudulent accounts and tax returns were filed in their names.”); see also In re Yahoo! Inc. Customer Data Sec. Breach Litig., No. 16-MD-02752-LHK, 2017 WL 3727318, at \*14 (N.D. Cal. Aug. 30, 2017) (finding that the plaintiffs plausibly alleged injury in the form of diminution in value of PII when it was alleged that the PII was actually used by hackers); In re Experian Data Breach Litig., No. SACV 15-1592 AG, 2016 WL 7973595, at \*5 (C.D. Cal. Dec. 29, 2016) (finding that the plaintiffs sufficiently alleged damages when they alleged they had received “text messages from an apparent hacker” traced to the data breach at issue). Accordingly, the allegations of injury in the form of damage to and diminution in the value of Plaintiff’s PII are not sufficient to constitute injury-in-fact.

#### **b. Loss of Privacy**

Plaintiff also alleges injury in the form of loss of privacy from the exposure of his PII. (Doc. No. 1, p. 7). However, the factual allegations related to this asserted injury suffer from the same deficiencies described above. Plaintiff alleges nothing more than the “mere compromise” of his PII and a resulting loss of privacy, which is too abstract of an injury to satisfy standing requirements. See Khan v. Child.’s Nat’l Health Sys., 188 F. Supp. 3d 524, 533 (D. Md. 2016) (holding that an injury described as a “data breach [that] caused a loss of privacy” was not a “concrete and particularized injury” (quoting In re Zappos.com, Inc., 108 F. Supp. 3d 949, 962 n.5 (D. Nev. 2015))); see also O’Shea v. Littleton, 414 U.S. 488, 494, 94 S. Ct. 669, 675, 38 L. Ed 2d 674 (1974) (“Abstract injury is not enough.”). The Court has been unable to find any law holding otherwise in the data breach context, and Plaintiff has not provided any. The Complaint accordingly fails to sufficiently allege that Plaintiff’s loss of privacy constitutes an injury-in-fact.

**c. Increased Risk of Fraud and Identity Theft and Mitigating Measures**

Finally, Plaintiff asserts he has been injured because the exposure of his PII has left him with the “imminent and impending [risk] of fraud and identity theft.” (Doc. No. 1, p. 7). In addition to the continuing risk of harm from identity theft, Plaintiff also claims he has spent “time routinely reviewing his credit monitoring service results and reports. Id. Ultimately, Plaintiff’s third alleged injury has two prongs: (1) the injury resulting from being at increased risk of identity theft and (2) the injury resulting from the time spent on mitigative measures to protect against the increased risk of identity theft.

In light of Beck and Hutton, it is clear that Plaintiff has not suffered an injury-in-fact for either the increased risk of future identity theft or the cost of mitigative measures, at least to the extent the injury is premised on the accidental data breach. With respect to the accidental breach, Plaintiff has neither alleged actual misuse of his PII, nor has he alleged his PII was intentionally targeted. Accordingly, to the extent any injury or allegation is based on the accidental data breach, Plaintiff has not sufficiently alleged injury-in-fact.

However, the question of whether Plaintiff has alleged injury-in-fact flowing from the alleged phishing scam requires a more nuanced analysis because, as Plaintiff argues in his Opposition Motion, all “phishing attempts” are “attacks by a thief with nefarious intentions.” (Doc. No. 13, p. 6). In highlighting this argument, Plaintiff agrees with the holding in Beck and argues he has satisfied its standard by pointing out that he has alleged “his . . . PII was intentionally targeted.” (Doc. No. 13, pp. 5-6).

First, the Court notes that the Complaint does *not* contain allegations that Plaintiff's PII was intentionally targeted in the alleged phishing scam.<sup>8</sup> See (Doc. No. 1). In his Opposition Motion, Plaintiff appears to ask this Court to instead *assume* that his PII was intentionally targeted simply because Defendant's employee was the victim of a phishing scam. See (Doc. No. 13). The Court agrees that most, if not all, phishing attempts are intended to achieve "nefarious" ends—but to assume the specific phishing attempt here was intended to target Plaintiff's PII is to engage in the same attenuated chain of possibilities explicitly rejected by the 4<sup>th</sup> Circuit in Beck.

To illustrate this attenuated chain of possibilities based on the factual allegations in the Complaint, which are taken as true, the Court must assume the following: (1) the phishing attempt intentionally targeted the PII belonging to Defendant's clients rather than other information potentially stored on Defendant's servers; (2) the reactionary steps taken by Defendant in an effort to protect against the phishing attempt failed, and clients' PII was taken by hackers;<sup>9</sup> (3) Plaintiff's PII was among the PII taken by the hackers; and (4), hackers have attempted or will attempt to use Plaintiff's, as opposed to anyone else's, PII to steal his identity.<sup>10</sup> This chain of assumptions tracks almost exactly with the attenuated chain explicitly rejected in Beck, except the one here has the additional assumption that Defendant's actions taken in response to the phishing attempt failed to stop the attack before any PII was taken. Thus, the Court struggles to see how the allegations in the Complaint are sufficient to satisfy the injury-in-fact requirement.

---

<sup>8</sup> The Complaint's allegations regarding the theft of Plaintiff's PII amount to conclusory statements, which need not be taken as true. See Beck, 848 F.3d at 270 ("We do not, however, apply the same presumption of truth to 'conclusory statements' and 'legal conclusions' contained in [the] complaint.").

<sup>9</sup> The Complaint makes clear that Defendants "took immediate action" upon learning about the phishing attempt and "blocked the unauthorized access, changed passwords and launched an investigation." (Doc. No. 1, p. 6).

<sup>10</sup> Although Plaintiff need not have suffered any actual identity theft to have sufficiently alleged injury-in-fact, there must be some factual allegation suggesting that hackers will use Plaintiff's PII to commit fraud.


Second, even Plaintiff's own Complaint belies the notion that he is at imminent and/or substantial risk of harm. To be sure, Plaintiff repeatedly asserts—in conclusory fashion—that he has been placed at “imminent, immediate, and continuing increased risk of harm” because of the data breaches. See (Doc. No. 1, pp. 7, 13). However, his Complaint also explains that he is at risk of injury “for years to come” and that “the fraudulent activity resulting from the Data breaches may not come to light for years.” Id. at pp. 8, 1. If what Plaintiff alleges is true, and fraudulent activity may not occur for *years*, it is impossible for him to be at imminent risk of harm.

Ultimately, what Plaintiff has alleged here amounts to nothing more than the “mere compromise” of personal information, notwithstanding the allegations that Plaintiff's PII was exposed after a phishing attack. See Kimbriel, 2019 WL 4861168, at \*3 (holding that plaintiffs' alleged injury of increased risk of future identity theft was too speculative and could not confer standing because the only facts alleged were “credit inquiries” tied to a phishing attack). And, as explained in detail above, *supra* Section III.a, Plaintiff has not alleged *anything* more than the “mere compromise” of his PII. Accordingly, Plaintiff has not sufficiently alleged injury-in-fact as required for Article III standing. Because the standing issue is dispositive, the Court declines to address Defendant's argument that Plaintiff has failed to state a claim.

#### IV. CONCLUSION

IT IS THEREFORE ORDERED Defendant's Motion to Dismiss (Doc. No. 12) is GRANTED and Plaintiff's Complaint is DISMISSED WITHOUT PREJUDICE. The Court respectfully directs the Clerk of Court to CLOSE this case.

Signed: March 24, 2021 IT IS SO ORDERED.

  
Frank D. Whitney  
United States District Judge

